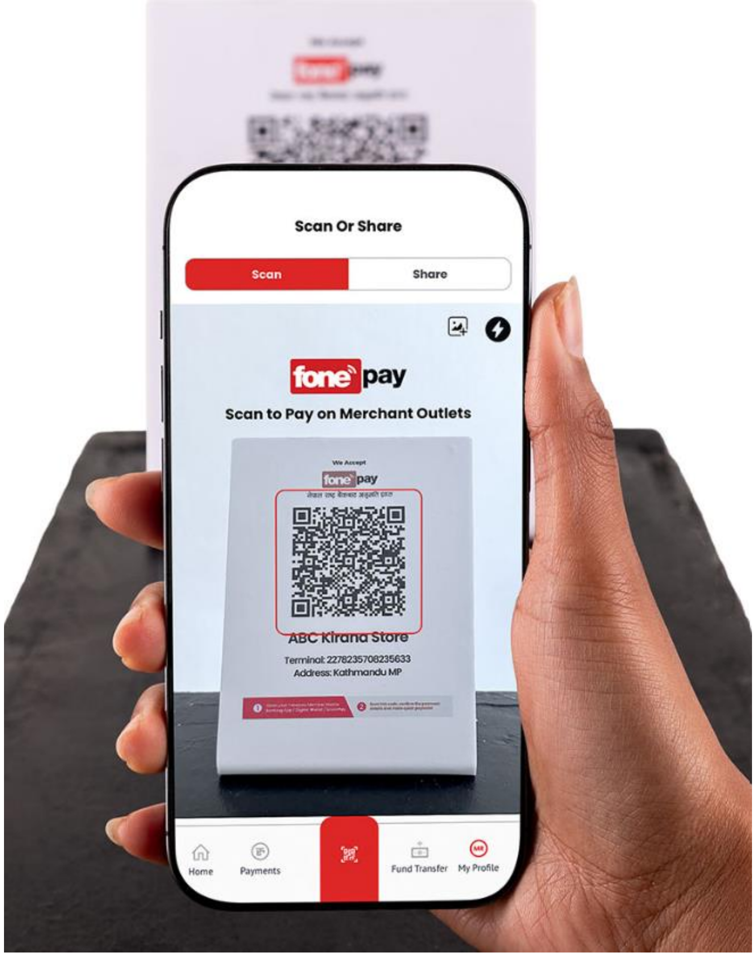


Merchant Onboarding Best Practices

Customer experience, Operational Efficiency and Risk Management

Abbreviations

S.N.	Abbreviations	Full Form
1	AML	Anti-Money Laundering
2	PCI DSS	Payment Card Industry Data Security Standard
3	PEPs	Politically Exposed Persons
4	PAN	Permanent Account Number
5	PSPs	Payment Service providers
6	QR	Quick Response
7	KYC	Know Your Customer
8	KYM	Know Your Merchant
9	NRB	Nepal Rastra Bank
10	MCC	Merchant Category Code
11	ISO	International Standard Organization
12	ID	Identity
13	CFT	Combating the Financing of Terrorism
14	CDD	Customer Due Diligence
15	STR	Suspicious Transaction Reporting
16	TTR	Threshold Transaction Reporting

Contents

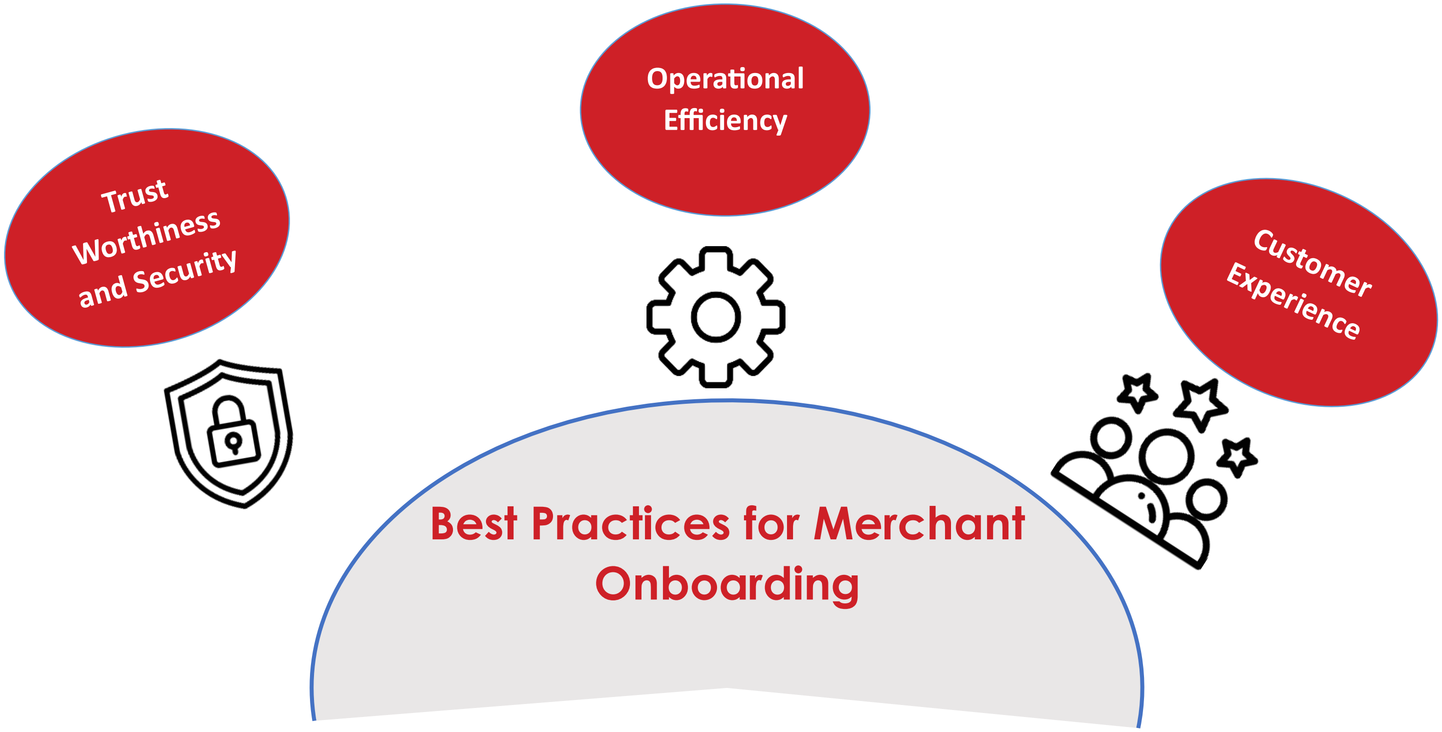
INTRODUCTION

Effortless Onboarding for Secure Payments, Enhancing Customer Experience and Operational Efficiency

Merchant onboarding is the process through which a payment service provider (PSP) enables a business to accept and manage customer payments securely. Implementing standardized onboarding practices is essential to ensure a smooth, efficient, and secure experience for new merchants. It helps reduce operational risks, enhance customer experience, and maintain compliance with regulatory requirements.

When a new merchant partners with a bank or PSP, they shall provide their personal and business information. It is essential to handle this information carefully to ensure a smooth and efficient onboarding process, which is critical for a positive merchant experience. Proper execution of the onboarding process helps establish a secure and effective payment setup from the start.

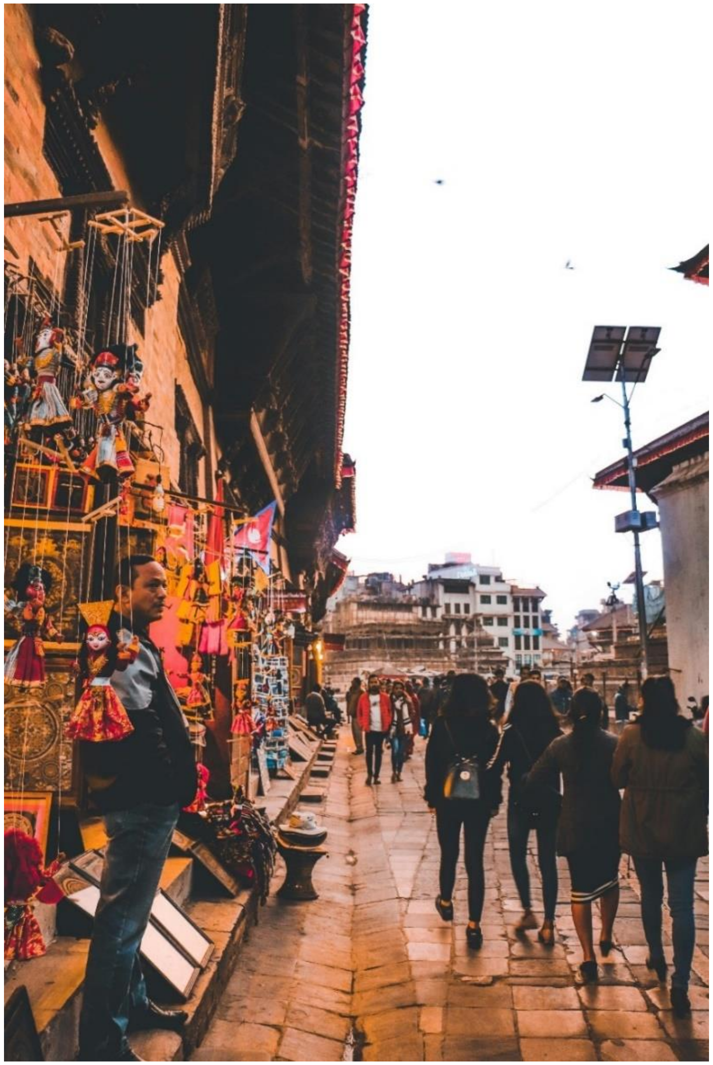
DEFINING OBJECTIVES


Operational Efficiency
Trust Worthiness and Security
Customer Experience
Best Practices for Merchant Onboarding

Key Objectives

1. Is it to streamline merchant and payment gateway?
2. Is it to make good operational efficiency?
3. Is it to make safe and secure platform for merchants?

TOOLS FOR MERCHANT RISK ASSESSMENT AND MANAGEMENT



1) Merchant Underwriting

Merchant underwriting is the process of assessing potential merchants to identify and manage risks before they enter the payments system. It involves verifying the merchant's identity, business model, and financial stability to ensure they comply with banking, legal, and security standards. This process helps prevent fraud and illegal activities by ensuring only legitimate businesses are allowed to accept payments. By thoroughly reviewing merchant applications, underwriting provides a strong foundation for understanding each business and maintaining a secure and reliable payments ecosystem.

2) Merchant Monitoring

Merchant monitoring continuously evaluates merchant risk using automated tools, human analysis, and machine learning. It identifies shifts in business models or tactics that may increase risk, such as accidental violations or fraudulent activities like transaction laundering, helping prevent fraud and mitigate high-risk behavior.

i) **Business Monitoring:** Continuously monitor merchants to ensure business activities match onboarding disclosures and comply with regulations.

ii) **Transaction Monitoring:** Detect and prevent unauthorized transaction to protect against fraud and illegal activities.

iii) **Regulatory Monitoring:** Stay updated on legal changes and ensure compliance with all relevant regulations.

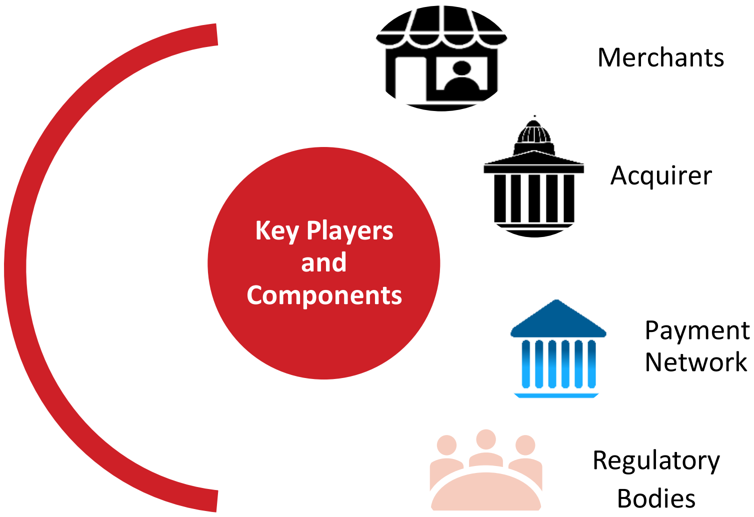
KEY PLAYERS AND COMPONENTS

Visions are realized under multiple eyes

BANK_ALERT
50,000.00 deposited in your A/C on 12/12/2023 14:16. Re: Sapati Return, Sadichha. Balance now: 87532.00

For the merchant onboarding process to be smooth and successful, it requires the coordination of multiple entities, including the merchant, payment service providers, networks, acquirer, and regulatory bodies.

- Merchants
- Acquirer
- Payment Network
- Regulatory Bodies



Key Players and Components

Merchants

Acquirer

Payment Network

Regulatory Bodies

Merchants

Merchants are businesses, retailers, or service providers that sell products or services and need to accept payments from customers. They establish relationships with various parties involved in transaction channels, which may include online, in-store, or mobile payments

Payment Network

A payment network is a system of interconnected financial entities, enabling the transfer of funds between individuals, businesses, or institutions. It involves participants like: banks, and other financial institutions linked by an electronic network, governed by shared regulations and managed by an association of members.

Acquirer

Acquirer are financial institutions that process and settle transactions on behalf of businesses. They serve as the intermediary for merchants, providing various branches for points of contact. These banks manage the risks associated with businesses, ensure compliance, and oversee merchant accounts.

Regulatory Bodies

Regulatory bodies ensure seamless operation of payment networks by enforcing compliance with regulations, adhering to payment network policies, and fostering secure, standardized practices.

MEMBERS RESPONSIBILITIES

As an acquirer are responsible for onboarding merchants onto the Fonepay Network, it's essential to adhere to Fonepay's guidelines and regulatory requirements set forth by Nepal Rastra Bank (NRB), Central Bank of Nepal following the Nepal QR Standardization Framework and Guidelines.

To ensure compliance and network integrity, implement these actions:

- ✓ Perform due diligence, including Know Your Merchant (KYM) checks and site visits, to verify merchant legitimacy and compliance before allowing transactions.
- ✓ Offer thorough training to merchants on KYC and onboarding guidelines to ensure compliance and secure transactions.

MERCHANT ONBORDING AND MONITORING PROCESS

The merchant onboarding process is vital, providing merchants with the necessary infrastructure for transactions, especially in e-commerce or retail settings. It encompasses identity verification, compliance checks, configuring payment systems, and upholding security standards. Essentially, the onboarding process for merchants should align seamlessly with payment service providers (PSPs)

Step 1: Payment Processor Pre-Screening

Step 2: Identify Verification/KYM

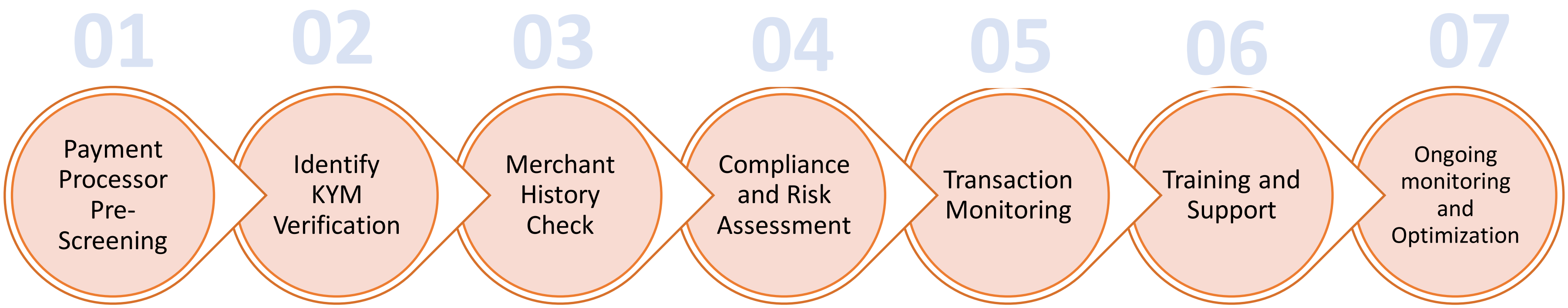
Step 3: Merchant History Check

Step 4: Compliance and Risk Assessment

Step 5: Transaction Monitoring

Step 6: Training and Support

Step 7: Ongoing monitoring and Optimization


01
Payment Processor Pre-Screening
02
Identify KYM Verification
03
Merchant History Check
04
Compliance and Risk Assessment
05
Transaction Monitoring
06
Training and Support
07
Ongoing monitoring and Optimization

1. Payment Processor Pre-Screening

✓ Pre-screening is the first stage in merchant onboarding.

✓ The payment service provider (PSP) collects basic information from the merchant.

✓ The PSP verifies the merchant's legitimacy and checks for any involvement in fraudulent activities.

✓ This initial phase sets the foundation for further due diligence and evaluation during the onboarding process.

2. Identify KYM Verification

✓ KYM Verification is essential for background checks during merchant onboarding.

✓ It helps prevent unauthorized access and builds trust between businesses and payment platforms.

✓ Many PSPs and acquirer use automated procedures to streamline the KYM process.

3. Merchant History Check

✓ Merchant History Check involves verifying the accuracy of the merchant's submitted documents.

✓ The PSP and acquirer screen the business and owners against databases for PEPs, AML, financial crimes, and corruption.

✓ Additional business information, such as registration licenses, shareholder data, financial statements, and industry details, is collected.

✓ Key details like PAN, contact number, account info, business name, and registration forms are cross-verified to confirm the merchant's legitimacy.

4. Compliance and Risk Assessment

- ✓ Merchants pose inherent risks that require careful evaluation.
- ✓ Key factors include business type, transaction volume, and credit history.
- ✓ Compliance with regulations and industry standards is assessed.
- ✓ The process helps identify and mitigate potential risks.

5. Transaction Monitoring

- ✓ Regularly assesses customer transactions for high-risk activities.
- ✓ Analyzes user backgrounds and financial profiles in real-time.
- ✓ Detects suspicious transactions and generates Suspicious Activity Reports (SARs).
- ✓ Supports anti-money laundering (AML) efforts by identifying illicit activities such as terrorism, arms trading, and human trafficking.

6. Training and Support

- ✓ PSPs and acquirer provide ongoing training and support.
- ✓ Training covers payment transactions, dispute handling, and compliance.
- ✓ Ensures the process runs smoothly and merchants follow regulations.

7. Ongoing monitoring and Optimization

- ✓ Continuously monitor merchant transactions and activities after training.
- ✓ Track changes like new products or business models that may require updates.
- ✓ Implement new fraud prevention measures and adjust systems as needed.

Efficiency and Effectiveness of the Merchant Onboarding Process

Onboarding Checklist

i) Prescreening to ensure validity of registration
ii) Identity verification/KYM
iii) Merchant history check
iv) Business review of merchant
v) Web content analysis for web-based merchants
vi) Assurance that the merchant shall keep customer data confidential
vii) Credit risk underwriting
viii) Merchant agreement

For online merchants, conduct a thorough review of their network security, encryption protocols, access controls, and adherence to industry standards such as PCI DSS.

Thorough Screening: Request additional documents for a rigorous merchant screening process to maintain platform integrity and reduce risks.

Simplified Application: Create an easy, intuitive application with progressive forms focusing on essential details.

Secure Submission: Set up a safe portal for document uploads, with clear guidelines and quick feedback.

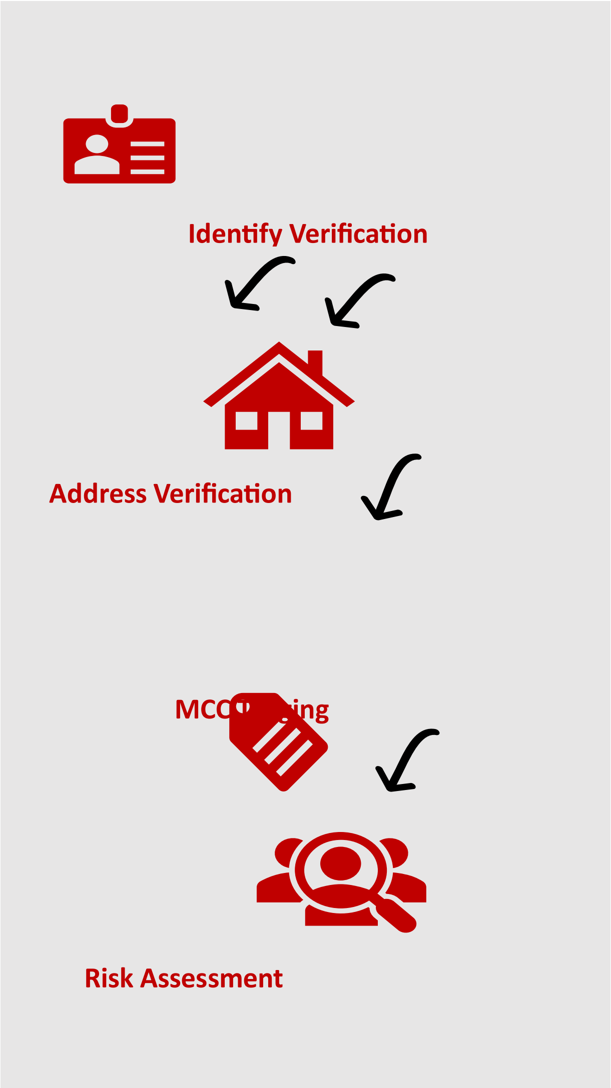
Real-time Updates: Provide merchants with automated notifications and status tracking throughout onboarding.

Training Support: Offer accessible tutorials and resources to help merchants navigate the payment system and troubleshoot issues.

Compliance and Security: Ensure onboarding meets regulatory standards with strong identity verification and fraud prevention.

Fast Payment Integration: Seamlessly link onboarding with payment systems to allow prompt payment acceptance.

Know Your Merchant



Understand what your customers value most and identify your company's strengths

Know Your Merchant

Know Your Merchant (KYM) is a comprehensive process that includes verifying the merchant's identity and address to ensure authenticity, classifying the merchant using Merchant Category Codes (MCC) to categorize the type of goods or services offered, and conducting a thorough risk assessment to evaluate potential financial and operational risks, thereby ensuring the integrity and security of transactions and compliance with regulatory requirements.

1. Identity Verification

Collect official documents in order to make sure the merchant's identity.

At least these essential Documents for the Merchant Onboarding Process:

- ✓ Business Registration Certificate
- ✓ Identity Verification/KYM
- ✓ Proof of Business Address
- ✓ Bank Account Details
- ✓ Government-Issued ID of Business Owners
- ✓ Shareholder Information
- ✓ Financial Statements
- ✓ Business Plan
- ✓ Merchant's Website or Online Presence (if applicable)
- ✓ Licenses and Permits (if applicable)

2. Address Verification

Verifying the address is crucial, as some merchants may operate non-existent or purely virtual shops. In any suspicious cases, banks or the relevant department must conduct physical visits to confirm the merchant's presence.

- A current utility bill (such as gas, electricity, telephone or mobile phone bill)
- A document issued by a government department that shows the End-user's address
- A bank statement (no older than 3 months) that shows the End-user's address.

3. MCC Tagging

Merchant Category Codes (MCC) are four-digit numbers assigned to merchants based on their primary business type, transaction nature, and services provided. These codes adhere to the ISO Standard, which offers a consistent list of MCCs along with their corresponding descriptions. Fonepay adheres to globally recognized MCC categorization standards, in line with International Payment Networks, Financial Institutions, and the guidelines set by Nepal Rastra Bank.

4. Risk Assessment

Merchant risk assessment is a crucial procedure for financial service providers engaged in payment processing, lending, or related services to merchants. Its primary goal is to recognize and manage potential risks such as fraud, credit issues, compliance issues, and operational challenges within the merchant portfolio.

Before and after the merchant onboarding process, shall consider at least these following points:

1) Collect and analyze data on business models, products, services, sales channels, target markets, financials, and customer feedback. Verify identity, ownership, location, and legal status.
2) Track sales volume, chargeback and refund rates, fraud incidents, customer complaints, and other risk indicators. Be vigilant for warning signs such as sales fluctuations, unusual payment patterns, negative reviews, or compliance issues.
3) Fulfill basic legal requirements and identify additional due diligence needs. Include fraud checks and ID verification in merchant assessments for thorough scrutiny.

Stay Secure, Stay Vigilant: Onboard with Confidence, Monitor with Precision

- ✓ **Compliance checks** ensure merchants adhere to regulatory standards and maintain operational integrity.
- ✓ **Transaction monitoring** helps detect fraud and ensures compliance with AML (Anti-Money Laundering) and CFT (Countering the Financing of Terrorism) laws.
- ✓ **Customer Due Diligence (CDD)** tools, including KYM (Know Your Merchant), verify merchant legality and assess risk.
- ✓ **CDD** tools also enable the reporting of suspicious activities to regulatory authorities.

Ensure Compliance, Build Trust, Drive Secure Transactions

Transaction Monitoring

Transaction monitoring serves dual purposes: detecting potentially fraudulent activity and ensuring regulatory compliance. Financial institutions are legally obligated to adopt rigorous anti-money laundering (AML) and counter-terrorist financing (CTF) measures, including robust transaction monitoring systems, to meet regulatory standards effectively.

Customer Due Diligence (CDD)

Customer Due Diligence (CDD) tools help financial institutions verify the legality of customers and assess associated risks. They involve implementing Know Your Merchant (KYM) practices, which include requesting identification and funding source documentation, conducting background checks, and evaluating a merchant's risk profile.

Compliance Checks

Compliance checks are a pivotal component of the merchant onboarding process, serving to verify adherence to comprehensive regulatory standards prior to merchants commencing transactions. This phase holds particular significance in regulatory environment, where strict compliance with laws and guidelines profoundly influences the operational legitimacy and reputational integrity of both merchants and the platforms facilitating the activities.

Risk Reporting Tools

Acquirer can generate and submit regulatory reports related to AML responsibilities using reporting tools. The reports, such as Suspicious Transaction Reports (STR) and Threshold Transaction Report (TTR), are sent to regulatory authorities upon detecting suspicious activities.

CHALLENGES AND SOLUTIONS WHILE ONBOARDING MERCHANT

Fraud Prevention

Challenge: Verifying the legitimacy of merchants can be challenging, and fraudulent merchants can slip through the cracks.

Solution: Implement advanced fraud detection mechanisms, including identity verification, transaction monitoring, and machine learning algorithms.

Data Security

Challenge: Handling sensitive merchant data requires top-notch security measures to protect against data breaches.

Solution: Invest in robust data encryption, secure storage, and regular security audits to fortify your data security.

Communication Gaps

Challenge: Inadequate communication can lead to misunderstandings and delays.

Solution: Set up a robust communication system that includes automated notifications, real-time chat support, and a dedicated support team.

Regulatory Compliance

Challenge: Navigating the complex landscape of financial regulations and compliance can be overwhelming.

Solution: Stay updated on relevant regulations and work with legal experts to ensure your onboarding process is compliant.

Long Onboarding Times

Challenge: Lengthy onboarding processes can frustrate merchants and lead to abandonment.

Solution: Continuously optimize your process to reduce unnecessary steps and automate wherever possible to expedite onboarding.